Anatomie útoku

Jak nás ohrožují hackeři a jak se můžeme bránit

Kybernetický útok může firmu přijít na miliony. Máte plán, jak útoku čelit, mírnit jeho následky a zotavit se z něj?

Microsoft

Obsah

03 **Úvod:**
Čtyři fáze útoku

04 **Fáze 1:**
První kroky k invazi

05 **Příklad z praxe:**
Služby

07 **Fáze 2:**
Přebírání moci

08 **Příklad z praxe:**
Média a zábavní průmysl

10 **Příklad z praxe:**
Potravinářství

12 **Fáze 3:**
Vstup do sítě

13 **Příklad z praxe:**
Vládní instituce

15 **Fáze 4:**
Dlouhodobá okupace

16 **Příklad z praxe:**
Hi-tech výroba

18 **Příklad z praxe:**
Internetový obchod

20 **Závěr:**
Ochrana, detekce, reakce

Úvod

Čtyři fáze útoku

Čtyři fáze útoku

Nebezpečí hrozí neustále. Kybernetické útoky přicházejí nečekaně a způsobují milionové škody na firemním majetku i reputaci. Máte představu, co vaší firmě hrozí? A máte nějaký plán, jak případnému útoku a jeho čtyřem fázím čelit, mírnit jeho následky a zotavit se z něj?

V této příručce se dozvíte více o průběhu útoku a také se seznámíte s několika příklady z praxe. Ty ukazují, jakou škodu útočníci v jednotlivých fázích působí. A především se naučíte, jak vytvořit obrannou strategii založenou na předvídání útoku, abyste mohli účinně chránit firmu i sebe.

Fáze 1:
První kroky k průniku

Fáze 2:
Přebírání zvýšených oprávnění

Fáze 3:
Útok se šíří do dalších systémů

Fáze 4:
Dlouhodobé ovládnutí sítě

Fáze 1: První kroky k průniku

K tomu, aby útočník pronikl do vaší firmy, stačí jediná chybička v obraně. Slabým článkem řetězu může být nechráněný počítač, špatně zabezpečený internetový server, zařízení cizího člověka s nesprávným nastavením a podobně. To vše pro útočníky představuje vítanou příležitost prolomit vaše ochranné mechanismy a proniknout k vám do firemní sítě. A jakmile se tam dostanou, začnou se rozhlížet kolem a vezmou si na mušku nejcennější informace, případně finance.

Slovníček:

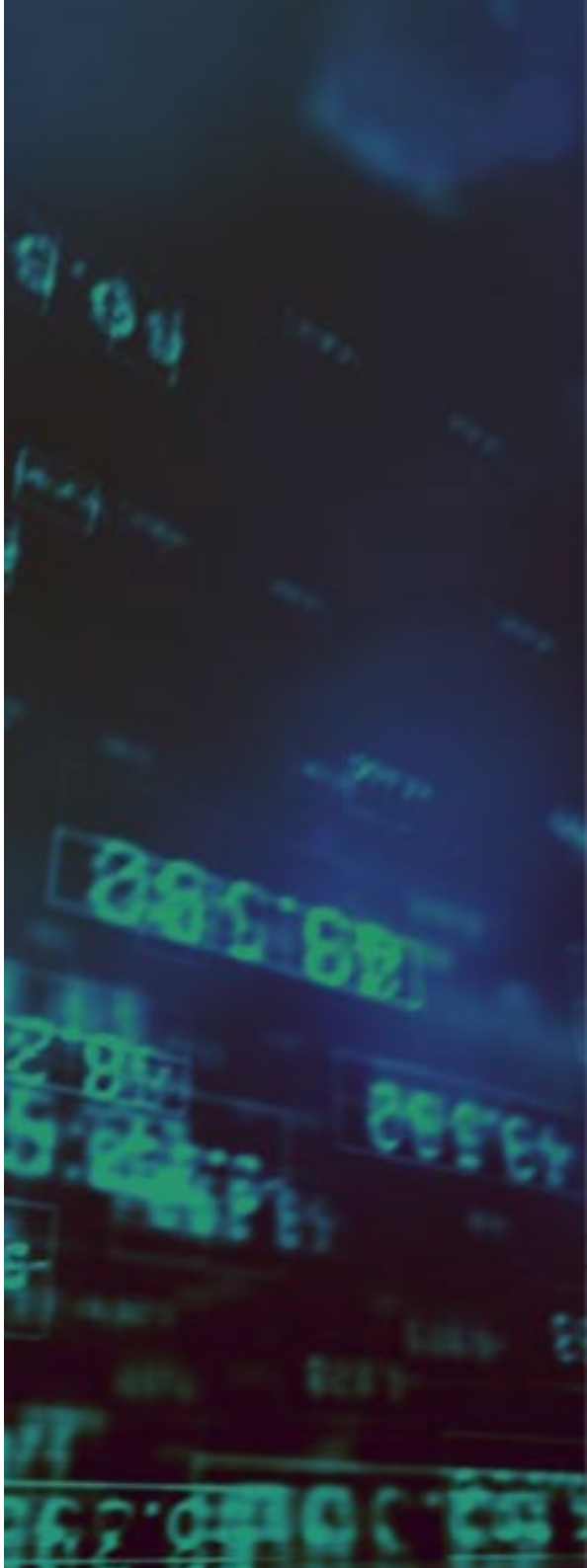
Phishing: Způsob, jak z uživatele podvodně vylákat osobní, finanční či firemní důvěrné informace, s nimiž je pak možné neoprávněně proniknout do vnitřní infrastruktury. Útočníci často používají falešné webové stránky nebo e-maily, které se tváří jako zprávy od důvěryhodných kontaktů (např. od obchodních partnerů nebo zaměstnanců). Cílem je přimět adresáta, aby klikl na webový odkaz se škodlivým obsahem, otevřel infikovaný dokument apod.

Watering hole: Další oblíbený typ útoku. Útočník zjistí, že potenciální oběť často navštěvuje určitou webovou stránku. Následně na tuto stránku umístí malware čili škodlivý obsah a doufá, že se uživatel při příští návštěvě „nakazí".

Malware: Zkrácený termín pro škodlivý (anglicky malicious) software. Souhrnné označení pro programy, které na vašem počítači provádějí něco nekalého – kradou informace, zamknou počítač a vyžadují výkupné, případně využijí počítač k rozesílání spamů. Mezi malware patří viry, červi nebo trojské koně. (V tomto dokumentu se zaměřujeme především na tzv. cílený malware, tedy škodlivé programy určené k průniku do konkrétního oboru či organizace).

Exploit: Část kódu, která využívá chyby v zabezpečení softwaru a krade z vašeho počítače informace, případně do něj instaluje malware.

Zero day: Chyba v zabezpečení software, která se výrobci softwaru ještě nepodařilo odhalit nebo opravit a kterou využívají exploity k získání přístupu k počítači nebo infrastruktuře. Někdy také zranitelnost nultého dne.



Příklad z praxe: Služby

Poskytování služeb se v posledních letech výrazně konsolidovalo, což souvisí se slučováním jednotlivých firem do holdingů. Z hlediska fungování celého ekosystému firem byla konsolidace bezpochyby úspěšná, na pracovníky jednotlivých firem ovšem celý proces slučování klade značné technické nároky. Nové komplexy se často snaží snížit investice a náklady na informační technologie a sdružují tak veškeré IT služby do jediného centrálního oddělení.

Jestliže se při slučování sítí, infrastruktury a softwarových systémů nepostupuje s dostatečnou opatrností, mohou vznikat chyby v zabezpečení. Útočníci se většinou zaměří na síť, jejíž zabezpečení je nejslabší. A jakmile se dostanou dovnitř, mohou začít využívat interních bezpečnostních problémů a pronikat do dalších a dalších úrovní. Příklad z praxe: Útočník se dostal do jedné ze sítí a pak využil e-mail pro podvržení zprávy ze sociální sítě, aby pronikl do jiného systému jednoho prodejce plynu. Pracovníci firmy si problém uvědomili až ve chvíli, kdy po aktualizaci softwaru začalo docházet k nestabilnímu chování serverů. Následné šetření odhalilo škodlivý program, který byl v síti nainstalovaný již před drahnou dobou a rušil její zabezpečení.

Útok tehdy umožnila celá řada různých příčin. Firma například neoddělila svou centrální síť od jiných sítí dalších dceřiných firem, takže se do ní útočníci dostali pomocí jedné hůře zabezpečené. V celé síti fungovala jednotná úroveň oprávnění, jakmile tedy útočníci pronikli dovnitř, mohli se tu už pohybovat celkem volně. A vlastní, na míru programované, aplikace využívaly příliš otevřený systém oprávnění. Trvalo několik let, než se podařilo síť od základů změnit a zabezpečit, a také obnovit důvěru uživatelů.

Jakmile se útočníkům povede první krok, mají rázem mnohem lehčí práci. Dostanou-li se do sítě pomocí některé z těchto metod, mohou se v rámci systému pokusit získat vyšší oprávnění a proniknout do důležitějších a citlivějších částí síťové struktury.

Trocha prevence

K bezpečnějším sítím pomohou firmám v oblasti poskytování služeb lepší bezpečnostní opatření, k nimž patří i školení zaměstnanců a nasazení vhodných technologických řešení.

Doporučujeme následující preventivní opatření:

Především je zapotřebí zavést základní bezpečnostní standardy pro zařízení tohoto typu. Znamená to oddělit jednotlivé sítě, vyžadovat po uživatelích silná hesla, přidělovat uživatelům jen taková oprávnění, jaká skutečně potřebují k práci, a k přístupu do každé sítě či její části vyžadovat samostatné heslo. Tato opatření jsou obzvláště důležitá při práci se staršími zařízeními a aplikacemi, které jsou zranitelnější, ale přitom je nelze opravit.

Aktualizujte sítě. Snažte se vždy používat aktuální infrastrukturu, k níž patří i nejnovější verze bezpečnostních systémů a softwaru.

Využívejte řešení s vlastním zabezpečením. Cloudové služby Microsoftu vyhoví jakýmkoli nárokům moderních organizací, funkce Advanced Threat Protection ve Windows 10 a Office 365 automaticky prohlíží veškeré odkazy a přílohy v došlých e-mailech a hledá potenciálně závadný obsah. Podezřelé materiály se k adresátům vůbec nedostanou, takže se riziko pramenící z nesprávného chování na síti výrazně snižuje.

Fáze 2: Přebírání zvýšených oprávnění

Když se útočníkům podaří proniknout do organizace, přichází další krok – na lokální úrovni se pokoušejí dostat k vyšším úrovním oprávnění. Většinou se snaží buď převzít kontrolu nad lokálním systémem, nebo odtud proniknout do jiného systému, v němž mají lepší šanci na získání práv administrátorů, případně na přístup k cenným datům. K tomu potřebují zjistit, jaké uživatelské účty jsou zodpovědné za správu systému, a pak se za uživatele těchto účtů vydávat. Mohou tak spravovat, aktualizovat a využívat systémové zdroje. Pak útočníci s pomocí systémově dostupných i externě stažených nástrojů zjišťují, jaké jiné systémy a sítě by pro ně mohly být zajímavé, a pokoušejí se získat příslušná uživatelská jména a hesla. Podobné aktivity uživatel s normálními právy nemůže podnikat s úspěchem.

Slovníček

Keyloggery: Malware, který monitoruje psaní na klávesnici. Z následného záznamu psaných znaků dokážou útočníci vyčíst uživatelská jména a hesla, kterými se pak snadno dostanou na různá místa do sítě.

Pass the hash (PtH): Technika, při níž útočníci využívají tzv. hash kódu v hesle vybraného uživatele, a za tohoto uživatele se následně vydávají. Útočníci v takovém případě vůbec nemusejí znát přístupové údaje daného uživatele, příslušný server jim přístup povolí i bez nich.

Síťové skenování: Tuto průzkumnou metodu útočníci používají ke katalogizaci dostupných systémů (např. hostingových serverů, služeb a zdrojů, které jsou v dané síti aktivní). Pak si vytvoří seznam cílů, tedy atraktivních systémů, a pokusí se na ně proniknout s pomocí nově získaných přístupových údajů a práv.

Příklad z praxe: Média a zábavní průmysl

Vezměte obor, který přitahuje spoustu lidí, přidejte trochu kontroverzního obsahu, a máte dokonalý cíl pro hacktivisty (hackeři, kteří počítačové útoky spojují se společenskou angažovaností). Za útoky na média a showbyznys často stojí touha nejen ukrást cenné informace, ale zároveň tím dát veřejně najevo svůj postoj. Nedávné útoky hacktivistů končily zveřejněním citlivých informací o napadených společnostech, případně se útočníci zmocnili firemních webových stránek.

V jednom takovém případě útok nejenže znemožnil fungování jedné nejmenované společnosti, ale navíc došlo ke zveřejnění citlivých informací o firemních zaměstnancích, zákaznících i duševním vlastnictví. Dosud není úplně jasné, jak k útoku vlastně došlo, k podobným případům však velmi často vede kombinace známých příčin – problematické chování na sociálních sítích a na internetu obecně, neošetřená bezpečnostní rizika a špatná nastavení systémových parametrů.

Škody pro mediální společnost mohou být vskutku dalekosáhlé. V popsaném případě se jednalo o výjimečně závažný útok s bezprecedentními následky, co se týče finančních i nemateriálních ztrát. Kromě jasně vyčíslitelných nákladů na akutní řešení situace znamenal útok i obrovskou ránu pro reputaci dané společnosti. V současné době musí tato společnost vynakládat spoustu času a peněz na obnovení důvěry a bývalých vztahů, přitom by potřebovala investovat do nových projektů.

Úspěšné řešení

Ničivému útoku lze předcházet vytvořením lepší bezpečnostní strategie, jejíž nedílnou součástí je komplexní řízení rizik. K tomu je nutné vědět, jaká aktiva firma vlastní a spravuje, jaká rizika těmto aktivům hrozí, kolik bude stát případné narušení bezpečnosti a jakými nástroji firma v současné době tato aktiva chrání. Také je nesmírně důležité umět správně rozpoznat, že nastal problém, vyřešit ho a následně zvládnout i jeho důsledky. Vše by mělo probíhat na cyklické bázi – rizika je zapotřebí hodnotit neustále, při vývoji bezpečnostního systému je nutné brát v úvahu poučení z předchozích případů.

Doporučujeme vsadit na následující bezpečnostní opatření:

Ochrana, detekce, reakce. Tak by se dal definovat obecný rámec bezpečnostních systémů, který používá Microsoft i mnohé další firmy. Patří do něj analýza rizik, řešení případného útoku, obnovení žádoucího stavu i poučení z celé události.

Přidělujte uživatelům jen taková oprávnění, jaká skutečně potřebují k práci. Přístup je dobré povolovat jednotlivým zaměstnancům striktně podle jejich pracovního zařazení, nikoli podle individuální pracovní náplně. A oprávnění by mělo být omezené na minimální míru, s níž daný zaměstnanec může plnit své povinnosti. Pokud ke své práci nutně nepotřebuje přístup k určité síti nebo materiálům, nedávejte mu ho. Toto opatření patří k základním zásadám prevence útoků.

Security Development Lifecycle. Jde o proces vývoje softwaru, který vývojářům usnadňuje tvorbu bezpečnějších programů a řeší nejrůznější bezpečnostní požadavky, aniž by přitom rostly náklady na vývoj.

Dále doporučujeme použít následující nástroje:

Local Administrator Password Solutions (LAPS): Softwarové řešení, s jehož pomocí lze nastavit na každém počítači v rámci jedné domény jiné, náhodně generované heslo. Správci domény pak mohou určit, kteří uživatelé (např. administrátoři helpdesku) mají právo tato hesla číst.

Windows 10 Credential Guard: Bezpečnostní nástroj založený na principu virtualizace se poprvé představil v operačním systému Windows 10 Enterprise. Dokáže izolovat důvěrná data tak, že se k nim dostane jen systémový software s náležitým oprávněním.

Microsoft Advanced Threat Analytics (ATA): Tento nástroj pomáhá odhalit hrozby a útoky typu PtH metodou behaviorální analýzy. Řeší tak požadavky na bezpečnost systému bez nutnosti rozsáhlých investic.

Příklad z praxe: Potravinářství

Velký výrobce nápojů věděl, že potřebuje vylepšit síťové zabezpečení a zároveň snížit náklady na IT, a přemýšlel, kudy na to. Vedení společnosti se nakonec rozhodlo celé IT oddělení přesunout pod křídla externí firmy a soustředit se jen na hlavní náplň práce, tedy na výrobu osvěžujících nápojů. Outsourcing IT do specializované firmy měl mimo jiné zajistit lepší zabezpečení dat, potravinářské společnosti se to ovšem vůbec nevyplatilo. IT firma se ke svěřeným citlivým datům rozhodně nechovala s péčí řádného hospodáře, nedodržovala pracovní postupy stanovené pro tuto situaci. Zároveň nenastavila správný způsob ochrany účtů s vysokým oprávněním, jejichž uživatelé měli přístup na mimořádně důležité servery.

V tomto případě počítačová firma najatá na správu dat neoddělila účty potravinářské společnosti od svých vlastních účtů, čímž data klienta vystavila běžným útokům (např. pokusům o prolomení bezpečnosti prostřednictvím e-mailu počítačové firmy, případně nesprávným chováním na internetu). Jakmile se útočníci zmocnili účtů potravinářské společnosti, mohli je ovládat na dálku podobně jako pracovníci počítačové firmy. A aby toho nebylo málo, potravinářská společnost mohla komunikovat výhradně prostřednictvím správcovské firmy, protože už se v ní fyzicky nenacházely její vlastní páteřní IT systémy. Diagnostika, koordinace i náprava celé situace tak byla téměř nemožná, dokud se napadených účtů neujal tým specialistů na záchranu dat.

Celý původní problém bylo přitom možné řešit úplně jinak. Outsourcing se mohl týkat jen části důležitých procesů, nejdůležitější data a páteřní systémy si potravinářská společnost mohla ponechat. Ke snížení nákladů navíc nebyl outsourcing nutně zapotřebí, stačilo přesunout některé z obchodních systémů do cloudu (například bylo možné nahradit interní mailový server komplexním řešením typu Office 365) a soustředit se přitom na interní firemní procesy týkající se výroby nápojů. Zmíněné cloudové řešení uvolňuje ruce zaměstnancům, měsíční náklady lze snadno předvídat, data přitom zůstávají pevně v rukou společnosti a jejich majitel se nemusí zcela spoléhat na externí služby.

Jestliže firemní prostředí tvoří velké množství systémů a celá struktura už je příliš velká, doporučujeme zvážit přesun těchto systémů do důvěryhodné cloudové služby. Cloud umožňuje firmě zachovat si kompletní platformu, infrastrukturu a služby, a přitom se zbavit starostí s nastavením a údržbou systémů a datových center. Společnost zároveň nemusí řešit bezpečnostní aktualizace a administraci operačních systémů ani hardwaru.

Při outsourcingu i při přesunu systémů do cloudových služeb je dobré ptát se zástupců příslušných firem na jejich zásady a postupy v oblasti zabezpečení a správy dat, ochrany soukromí, dodržování platných předpisů i transparentnosti. Kdyby zmíněná potravinářská společnost předem odhalila rizika spojená s outsourcingem a bezpečnostními postupy vybrané firmy, mohla by se rozhodnout mnohem lépe, komu důležité systémy svěřit.

Recept na úspěch

Outsourcing IT systémů a služeb může vypadat atraktivně díky zřejmému snížení nákladů. Jenže je bezpodmínečně nutné položit si otázku, zda jde skutečně o nejlepší řešení z hlediska zabezpečení dat a duševního vlastnictví společnosti. A stejně tak je zapotřebí vybrat partnerskou firmu, jejímž zásadám a postupům důvěřujete. Vedle výhod outsourcingu musíte zvážit i riziko plynoucí z předání dat do cizích rukou, což se výše zmíněné potravinářské firmě vymstilo.

Ještě před oslovením externího partnera je dobré položit si následující otázky:

- **Jaké služby bychom měli přesunout do cizích rukou?**
- **Jakou úroveň oprávnění externímu partnerovi přidělit?**
- **Je možné místo outsourcingu zvolit jiné řešení pro úsporu nákladů – přesun dat a systémů do cloudu?**

Až si na tyto otázky odpovíte, můžete se definitivně rozhodnout, zda zvolit outsourcing nebo cloudové řešení. V obou případech je ovšem nutné potenciálního poskytovatele služeb pořádně prověřit. Kromě níže uvedených otázek doporučujeme zjistit, zda poskytuje záruku bezpečnosti i pro případ živelné pohromy.

Potenciálního partnera pro outsourcing se zeptejte na tyto otázky.

- **Řídíte se při práci s daty a systémy kodexem Enhanced Security Administrative Environment (ESAE)?**
- **Máte zavedená omezení ohledně přístupu z účtů pro doménového administrátora (DA) a podnikového administrátora (EA)?**
- **Používáte řešení Privileged Identity Management pro službu Active Directory Azure?**

Fáze 3: Útok se šíří do dalších systémů

Ve třetí fázi se útok šíří napadenou sítí z jednoho počítače nebo serveru do velkého množství systémů. Útočníci si následně vytvářejí podmínky pro opakovaný vstup – buď tzv. backdoor neboli stálá „zadní vrátka“, jimiž se dostanou dovnitř kdykoli, nebo jiný podobný mechanismus.

K tomu útočníci využívají různé nástroje. Někdy jde o malware, jindy se útok maskuje méně nápadně. Útočníci mohou například vytvořit falešný účet a jeho prostřednictvím získat oprávnění ke vstupu, díky čemuž mají k dispozici hned několik možností, jak do sítě proniknout, ukrýt se v ní a dostat se k nejrůznějším zdrojům. Při využití malwaru, kterému se v tomto případě zpravidla přezdívá „bot“, útočníci většinou spoléhají na řídící server (command and control, C&C), který jim umožňuje dálkově ovládat jimi zavedený malware.. Pokud zjistí, že se některý z jimi kontrolovaných přístupových bodů opakovaně odpojuje, je to pro ně varování, že je jim někdo na stopě. V takovém případě prostě přístupový bod změní, čímž se před pronásledovateli opět ukryjí.

Slovníček

Bot: Drobný skrytý program, který útočníci instalují na cizí počítač bez vědomí majitele (od slova robot).

Botnet: Škodlivý systém, v němž se na velké množství počítačů instalují kopie stejných botů. Hacker je pak ovládá najednou, čehož lze využít při rozsáhlých útocích.

Command and control (C&C): Systém tvořený řídícím serverem a infrastrukturou, který se používá k synchronnímu ovládání mnoha počítačů z jednoho centra. Slouží např. k řízení botnetů. Hacker, který takový systém ovládá, si říká botmaster.

Příklad z praxe: Vládní instituce

Vládní instituce, o níž je nyní řeč, postupovala skoro ve všem správně. Pravidelně a podle instrukcí aktualizovala software, administrátorská práva mělo relativně málo uživatelů, pravidelně probíhaly bezpečnostní kontroly. Navíc tu chvályhodně zřídili samostatné pracovní stanice pro doménového a podnikového administrátora. (Tito administrátoři, označovaní též zkratkami DA a EA, kontrolují všechny ostatní účty v rámci organizace. Takové oprávnění by ve firmě mělo mít jen minimum lidí a jeho přidělení by mělo podléhat přísné kontrole.)

Přesto došlo k osudové chybě – v personálním, finančním i IT oddělení se používalo stejné administrátorské heslo. Těžko pochopit, že inteligentní jedinci s přístupem k vládním informačním zdrojům mohou takovou hloupost vůbec udělat, ale stalo se.

Jednotná lokální administrátorská hesla se ve skutečnosti používají ve spoustě organizací, které vůbec netuší, jak riskantní to je. Důvody jsou různé – občas se třeba stane, že nastavení systémů při nízkých přístupových právech jednotlivých účtů nefunguje, jak by mělo. Administrátoři to řeší tím, že účtům přidělí dočasně vyšší práva, dokud vše nezačne fungovat správně. Když se ovšem problém vyřešit nedaří, ponechají administrátoři vyšší práva účtům natrvalo. Jindy zase jednotné heslo nastaví jako provizorní řešení při instalaci, poté na to zapomenou a heslo zůstane. V každém případě je takový systém otevřený útokům všeho druhu. Podobná nastavení svědčí o tom, že pracovníci IT oddělení přemýšlejí jen na lokální úrovni a neuvědomují si, jaká nebezpečí systémům hrozí při stálém připojení k internetu.

U tohoto vládního úřadu se útočníci do sítě dostali, když si jeden z uživatelů na svém počítači otevřel dokument nebo webovou stránku se škodlivým kódem (přesně se nezjistilo, o jakou z těchto dvou možností skutečně šlo). Vzhledem ke stejným heslům používaným v různých odděleních se útok okamžitě rozšířil na různá místa po síti a útočníci snadno získali i přístupová práva doménového a podnikového administrátora. A s těmito právy už šlo všechno jako po másle – útočníci mohli bez problémů implantovat škodlivé kódy do datových center, na servery i do systému Microsoft Exchange, takže spolehlivě infiltrovali celou síť. Organizace utrpěla škodu ve výši mnoha milionů dolarů.

A to hovoříme jen o škodě, která se dala vyčíslit – jde o náklady na obnovu systémů, vytvoření nových hesel a vyšetřování celého incidentu. Kolik ovšem nešťastnou vládní agenturu stála ztráta důvěry s napadením spojená, nikdo stanovit nedokáže.

Komplexní ochrana

Vládní instituce, o níž jsme hovořili, v mnohém postupovala správně. Úspěšná ochrana před útokem ovšem musí mít komplexní podobu.

Doporučujeme následující ochranné mechanismy:

Microsoft Enhanced Mitigation Experience Toolkit (EMET): Nástroj pro ochranu zranitelných míst v softwaru, aby je útočníci nemohli využít.

Microsoft Office 365: Kancelářská sada s dostatečnou úrovní ochrany pro firemní účely. Splňuje zákonné i technické požadavky na zabezpečení.

Enhanced Security Administrative Environment (ESAE): S pomocí vyspělých moderních technologií a doporučených postupů vytváří tento nástroj bezpečné prostředí s vysokou mírou ochrany pro administraci i běžnou práci.

Privileged Identity Management for Active Directory: Umožňuje spravovat, ovládat a sledovat účty s nadstandardními přístupovými právy a jejich přístup ke zdrojům pomocí nástroje Azure Active Directory a dalších online služeb Microsoftu (např. Office 365 nebo Microsoft Intune).

Microsoft Advanced Threat Analytics (ATA): Pomocí behaviorální analýzy monitoruje nestandardní chování účtů a využívání přístupových práv.

Operations Management Suite (OMS): Cloudové řešení pro IT management pomáhá monitorovat systém, upozornit na útok a stopovat útočníky.

Fáze 4: Dlouhodobé ovládnutí sítě

Ve čtvrté fázi se útočníci v síti usadí, zabydlí a připraví k dlouhodobému pobytu. Spouštějí malware, který nepřetržitě vyhledává mezery v zabezpečení a stahuje vybraná data, a zároveň se snaží co nejdéle zůstat v tajnosti. Vytvářejí si vlastní uživatelské účty, aby si v systému vybudovali bezpečnou pozici, a pravidelně mění hesla, aby unikli odhalení.

Podobně jako ve třetí fázi hackeři k opětovnému skrytému průniku do sítě používají infiltraci s pomocí malware, převážně boty. Svou pozici si zajišťují ovládnutím C&C a bez jakýchkoli překážek využívají síťové zdroje a kanály. A pokud mají podezření, že jejich přítomnost vyšla najevo, mají k dispozici nejrůznější nástroje, jak nevítané pozornosti uniknout a následně obnovit přístupová práva.

Slovníček

Advanced persistent threat (APT): Cílený útok na konkrétní cíl. Probíhá souvisle v určitém časovém úseku, útočníci se snaží zůstat v utajení a neoprávněně získat přístup k cizím datům.

Assume Breach: Doporučená strategie pro ochranu před útoky. Její podstatou nejsou pouhá preventivní opatření, ale komplexní přístup založený na detekci, reakci a následné nápravě škod. Hacker, který takový systém ovládá, si říká botmaster.

Příklad z praxe: Hi-tech výroba

Když je to zapotřebí, dokážou být hackeři překvapivě trpěliví. Po infiltraci do sítě se v ní často vyskytují dlouhé měsíce, aniž by je kdokoli odhalil. Během této doby předělávají nejrůznější systémy, falšují záznamy o přístupech a vylepšují útočné nástroje. Jedna společnost zaměřená na hi-tech výrobu měla takové nevítané hosty ve své síti nejméně rok a půl, než na to přišla. Za tu dobu útočníci úspěšně nasadili cílený malware na firemní server, na nějž firma ukládala v podstatě celé své duševní vlastnictví.

Útočníci měli tak pravidelně k dispozici firemní powerpointové prezentace, veškerou dokumentaci, rozvrhy projektů i detailní informace o výrobě. Ještě před objevením útoku z různých částí firemní sítě zmizelo velké množství dat týkajících se výzkumu a vývoje.

Jak se lépe chránit

Nikdo už dnes nezjistí, jak se útočníci do firemní sítě dostali. Z povahy útoku je jasné jen to, že se jim podařilo nějak získat práva k tomu, aby do systému nainstalovali malware.

Pro ochranu před útoky tohoto typu doporučujeme následující nástroje:

Advanced Threat Protection: Tato funkce kancelářské sady Office 365 automaticky kontroluje všechny přílohy a odkazy v došlých e-mailech a hledá potenciálně závadný obsah. Podezřelé materiály se k adresátům vůbec nedostanou a riziko pramenící z nesprávného chování na síti se tak výrazně snižuje.

Multi-factor authorization (MFA): Vyžaduje po uživatelích další ověření totožnosti, pouhé uživatelské jméno a heslo nestačí. Mezi možné způsoby ověření patří třeba telefonát nebo textová zpráva.

Azure Rights Management (Azure RMS): Ochrana dokumentů a e-mailů pomocí šifrování, ověřování totožnosti a autorizačních nástrojů. Funguje na různých typech zařízení – na počítačích, tabletech i chytrých telefonech.

Microsoft OneDrive: Cloudové úložiště chrání soubory hned několika způsoby. Soubory nikdy nelze sdílet s jinými uživateli, pokud je neuložíte do veřejné složky nebo je sami neoznačíte jako sdílené. Zabezpečení lze posílit vhodným heslem, případně je možné vylepšit ochranu stávajícího účtu u Microsoftu například zadáním druhé e-mailové adresy nebo bezpečnostní otázky. Ověření tak může být dvoustupňové.

Datová centra Microsoft: S vývojem firemního software i provozováním globálních online služeb má Microsoft desítky let zkušeností, našim bezpečnostním technologiím se tedy dá skutečně důvěřovat. Mimořádně bezpečná jsou i naše datacentra – nacházejí se v budovách postavených přímo pro tento účel, o bezpečnost se starají spolehlivé ploty, ochranná služba i soustavné kontroly. Ke vstupu opravňují pracovníky biometrické čipy, personál prochází pravidelným výcvikem a v případě nouze je možné servery okamžitě fyzicky zničit bez možnosti obnovy. Všechna datacentra jsou nepřetržitě monitorována, ověřování přístupových práv využívá kombinovaných metod včetně biometrického skenování. Ke komunikaci slouží interní síť odpojená od veřejného internetu.

Příklad z praxe: Internetový obchod

Poslední varovný příběh se odehrává na internetu.

O útocích na velké e-shopy, při nichž pachatelé cílili na citlivé informace o zákaznících, nejspíš už slyšel každý. Většina velkých internetových obchodů nabízí klíčovým obchodním partnerům (např. provozovatelům platebních karet) možnost vzdáleného přístupu do sítě s minimem omezení. V některých případech se tito partneři pohybují téměř na úrovni interních pracovníků. To je první varovné znamení. Druhým jsou pak nedostatečně oddělené sítě. Jinými slovy, pokud se někdo dostane dovnitř, může se po napadených firemních serverech pohybovat zcela svobodně.

Hned v několika případech se přitom útočníci dostali do systému právě prostřednictvím obchodních partnerů napadené firmy. Po nabourání do sítě se pachatel maskuje právě jako takový partner, zkoumá nejrůznější systémy a snaží se prolomit ochranu těch nejdůležitějších, tedy těch, na nichž se skrývají finanční informace. Případně se snaží použít uživatelský účet, který má k těmto informacím přístupová práva.
V praxi tedy hackeři napadli určitou firmu jen proto, aby tak získali přístup do firmy jiné, která s napadenou firmou obchoduje.

Již pár dní po takovém útoku mohou akcie a reputace napadených společností výrazně poklesnout. A to není vše, oběť útoku čeká i tvrdá pokuta od vlády, která může dosahovat až miliardových částek v dolarech, zvláště pokud se jedná o regulovaný obor se speciálními požadavky na zabezpečení. Pokuty nebo soudní spory se samozřejmě nemusejí vyhnout ani partnerské společnosti, která se ukázala jako nejslabší článek řetězu. Některým firmám proto stojí za to se proti takovým incidentům pojistit.

Ochrana při nákupech

Nejjistějším způsobem, jak se chránit před útokem prostřednictvím vzdáleného přístupu, je takový přístup prostě zakázat. Jenže to mnohé firmy udělat dost dobře nemohou, internetové obchody a služby nevyjímaje.

Několik bezpečných způsobů, jak umožnit partnerům přístup ke své síti:

Přesuňte aplikace do cloudu. Určité aplikace například transakční weby nebo databázové systémy, lze svěřit důvěryhodné cloudové platformě fungující jako služba (PaaS). K těmto částem systému by pak měla existovat jen velmi omezená přístupová práva, dostupná by měla být jen data potřebná k běžné práci. Tímto způsobem se omezí jak počet uživatelů s přístupem k firemní síti, tak i přístupová práva uživatelů. Každý má přístup jen k těm informacím, které skutečně potřebuje.

Několikastupňové ověření (multi-factor authorization, MFA). Uživatelské jméno a heslo nestačí, je zapotřebí ověřit totožnost uživatele i dalším způsobem. Poslouží třeba telefonát nebo textová zpráva.

Migrace ze vzdáleného přístupového bodu (RDP) k virtuálnímu zařízení (VM) v Azure. Virtuální zařízení umožňují nastavit unikátní hesla pro různé segmenty sítě a sledovat, kdo má přístup k informacím.

Závěr

Ochrana, detekce, reakce

Ochrana, detekce, reakce

Chcete zlepšit zabezpečení firemních dat? Doporučujeme komplexní přístup. Důležité je pochopit, co je příčinou úspěchu cílených útoků. Útokům nejde zabránit, lze se na ně pouze důkladně připravit. Firemní systémy nejsou dokonalé, hackeři na ně útočí pravidelně. Proto je dobré sledovat, kde se v zabezpečení objevují bolavá místa, a snažit se riziko maximálně omezit. A zároveň je zapotřebí mít plán, jak na případný cílený útok efektivně a rychle zareagovat.

Správná strategie má tři kroky.

Krok číslo 1: Ochrana

Opatrnosti není nikdy dost a přístupová práva má mít jen ten, kdo se bez nich neobejde. Položte si následující otázky:

- Opravdu tento člověk potřebuje přístup k těmto informacím?
- Vím přesně, kde má data jsou?
- Vím, kdo všechno k nim má přístup?
- Mám jistotu, že můj systém vyhovuje zákonným i technickým požadavkům?
- Mám v systému aktualizovaný software?

Krok číslo 2: Detekce

Vždy počítejte s tím, že k útoku dojde. Podezřívavost je v tomto případě na místě. Položte si následující otázky:

- Jak poznám, že došlo k útoku?
- Mám k dispozici vhodné nástroje pro detekci útoku?
- Mám k dispozici vhodné nástroje pro analýzu útoku?

Krok číslo 3: Reakce

Ověřte si, že máte plán, co v případě útoku dělat, a že máte i mechanismy, které tento plán v pravou chvíli spustí. Položte si následující otázky:

- Jak budeme na útok reagovat?
- Jak se vypořádáme se škodou na majetku a reputaci?
- Máme pro takový případ plán komunikace se zákazníky?
- Jak se z celé situace poučíme?

Společnost Microsoft pomáhá uchovat data v bezpečí a soukromí. Chcete-li vědět více o doporučených postupech a požadavcích v oblasti kybernetické bezpečnosti a ochrany soukromí, a zajímá-li vás, zda těmto požadavkům vyhovuje nastavení ve vaší firmě, navštivte stránky www.chranimedata.cz .

Tým Trusted Cloud děkuje všem, kteří se při přípravě této příručky podělili o svůj čas, znalosti a talent. Jmenovitě jsou to Bruce Cowper, Kasia Kaplinska, Matt Kemehar, IB Terry a Yvette Watersová.